Notice of Allowability	Application No.	Applicant(s)	
	09/741,217	SWANDER ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the c rrespondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/30/2004*.

2. ☒ The allowed claim(s) is/are *1-3,6-8 and 10-34*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 1/6/2005.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Examiner's Amendment

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it must be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Himanshu Amin on January 10, 2005.

1. The Examiner has contacted the Attorney of record, Himanshu Amin, to ask the Attorney if the Examiner could do an Examiner Amendment. Mr. Himanshu Amin agreed to incorporate claim 10 limitations into Independent claims 1, 16, 26-33.

2. As per claim 1, claim 10, which discloses "**wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users", is inserted into independent claim 1 after, "establish a secure link among users".**

3. Claim 10, is deleted.

4. As per Claim 16, the limitations of claim 10, "**wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users"**, is inserted after the words, "secure link among users", but immediately before the words, "wherein the subsystem generates".

5. As per Claim 26, the limitations of claim 10, "**wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure**

link among users", is inserted after a "secure link among users", but immediately before, "negotiating and authenticating".

6. As per claim 27, the limitations of claim 10, **"wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users"**, is inserted after the words, "a secure link among users", but immediately before the words, "negotiating and authenticating".

7. As per claim 28, the limitations of claim 10, **"wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users"**, is inserted after the words, "a secure link among users", but immediately before the words, "negotiating and authenticating".

8. As per claim 29, the limitations of claim 10, **"wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users"**, is inserted after the words, "a secure link among users", but immediately before the words, "negotiating and authenticating".

9. As per claims 30-33, the limitations of claim 10, **"wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users"**, should be inserted after, the words, "establish a secure link among users".

10. As per claim 10, has been canceled due to the incorporation of claim 10 into independent claims 1, 16, 26-33.

11. Thus, since claim 10 was incorporated into independent claims 1, 16, 26-33, then claims for which 10 depends now depends from 1. This claims include:

12. Claim 11, which discloses, "The system of claim 10", is changed to, "The system of claim 1".

13. Claim 12, which discloses, "The system of claim 11" is changed to, "The system of claim 1".

14. Claim 13, which discloses, "The system of claim 12", is to be changed to, "The system of claim 1".

15. Claim 14, which discloses, "The system of claim 11", is changed to, "The system of claim 1".

16. Claim 15, which discloses, "The system of claim 11", is changed to, "The system of claim 1".

Examiner's Statement

17. The Applicant is required to submit formal drawings.

Reasons For Allowance

18. The Examiner has searched patents as well as non-patent literature, the limitation that has been incorporated into independent claims 1, 16, 26-33, is allowed for the feature of, wherein the User mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users, is allowable, because in prior art as listed below: there are only to Modes, Main mode and quick mode. There is no third mode, or user mode, that utilizes

the keying material from Main mode negotiations. The Main mode, of prior art is responsible for negotiating keying material; there is no user mode that works with the Main mode.

19. In the prior art of Security, the limitations of, "the IKE module adapted to provide user mode negotiations in order to establish a secure link among users", and "establishing a secure link among multiple users on a single machine", and wherein the User mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users, is not disclosed or taught in prior art. In the prior art of security, specifically, Internet key exchange, there are two modes, main mode and quick mode. There is not disclosed of a user mode. The main mode also called phase I, is used to negotiate keying material for phase II, quick mode, that is IPSEC connection to secure datagrams. An example of prior art, that discloses phase I and II is Boden. However, Boden fails to disclose a user mode that provides negotiations in order to establish a secure link among users. The only two negotiation phases that are disclosed and taught in prior art of security are main mode and quick mode. Further, Boden discloses a one to one negotiation. The claimed invention calls for establish a secure link among users. Thus, the prior art of security fails to disclose the limitations above.

20. In the prior art of Networking, the limitations of, "the IKE module adapted to provide user mode negotiations in order to establish a secure link among users", and "establishing a secure link among multiple users on a single machine", is not disclosed or taught in prior art, is not disclosed or taught in prior art. An example of prior art that does not disclose this is, Harrison. Harrison discloses a security association is a relationship between a given set of network connections that establishes a set of shared security information. Harrison also discloses an IPSEC key management tunnel has two phases, phase I and II. Phase I/Main mode,

authenticate the entities, establishing a secret and parameters for the security association. Phase II/Quick Mode, exchanging identities. There is not disclosed or suggested a third phase or user mode.

21. In the prior art of key exchange, the limitations of, the IKE module adapted to provide user mode negotiations in order to establish a secure link among users," and "establishing a secure link among multiple users on a single machine, and "wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users, are not disclosed or taught by the prior art of key exchange. An example of prior art that does not disclose or suggest this, is Nikander. Nikander discloses the ISAKMP/Oakley Protocol, which uses the main mode and quick mode to establish secret and parameters for the security association, and exchanging identities. Prior art of key exchange fails to disclose the IKE module adapted to provide user mode negotiations in order to establish a secure link among users," and "establishing a secure link among multiple users on a single machine, and "wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users, are not disclosed or taught by the prior art of key exchange.

22. In non-patent literature, the limitations of, "the IKE module adapted to provide user mode negotiations in order to establish a secure link among users," and "establishing a secure link among multiple users on a single machine", is not disclosed or taught in non-patent literature. An example of non-patent literature that does not disclose this is Oakley Key Determination Protocol(RFC 2412). RFC 2412, teaches that the key exchange has a main mode and a quick mode. Further, RFC 2412, teaches how two parties can exchange keys, the initiator and

responder. Again, this is a one to one authentication of the parties, and also, there is no disclose or suggestion of a third mode or user mode. Thus, the non-patent literature fails to disclose the limitations above.

23. Another example of non-patent literature of Internet Society, that does not disclose or teach, the IKE module adapted to provide user mode negotiations in order to establish a secure link among users", and "establishing a secure link among multiple users on a single machine", is not disclosed or taught in non-patent literature. Internet Society teaches that Oakley defines a method to establish an authenticated key exchange. Oakley defines modes or phases. Phase I/Main mode is where two peers establish a secure authenticated channel with which to communicate. This is called a security association. Phase II/Quick mode, is where security associations are negotiated on behalf of services such as IPSec. There is not disclosed or suggested a third phase or user mode.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

January 6, 2005